This Page Is Inserted by IFW Operations
and is not a part of the Official Record

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

IMAGES ARE BEST AVAILABLE COPY.

As rescanning documents *will not* correct images, please do not report the images to the Image Problems Mailbox.

OIPE
JUL 2 8 2000
PATENT & TRADEMARK OFFICE
JC99

日 本 国 特 許 庁
PATENT OFFICE
JAPANESE GOVERNMENT

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日
Date of Application: １９９９年　５月１０日

出 願 番 号
Application Number: 平成１１年特許願第１２８１９７号

出 願 人
Applicant (s): 松下電器産業株式会社

RECEIVED
OCT -2 2000
TC 2700 MAIL ROOM

２０００年　３月　３日

特許庁長官
Commissioner,
Patent Office 近 藤 隆 彦

出証番号　出証特２０００－３０１２８６７

【書類名】　特許願

【整理番号】　2032410063

【提出日】　平成11年 5月10日

【あて先】　特許庁長官殿

【国際特許分類】　G11B 7/00

【発明者】

【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内

【氏名】　東海林　衛

【発明者】

【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内

【氏名】　大嶋　光昭

【発明者】

【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内

【氏名】　石田　隆

【発明者】

【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内

【氏名】　中村　敦史

【発明者】

【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内

【氏名】　謝花　正司

【発明者】

【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内

【氏名】　中田　浩平

【発明者】

【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内

【氏名】　大原　俊次

【特許出願人】

【識別番号】　000005821

【氏名又は名称】　松下電器産業株式会社

【代理人】

【識別番号】　100097445

【弁理士】

【氏名又は名称】　岩橋　文雄

【選任した代理人】

【識別番号】　100103355

【弁理士】

【氏名又は名称】　坂口　智康

【選任した代理人】

【識別番号】　100109667

【弁理士】

【氏名又は名称】　内藤　浩樹

【手数料の表示】

【予納台帳番号】　011305

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【包括委任状番号】　9809938

【プルーフの要否】　不要

【書類名】　明細書

【発明の名称】　暗号化コンテンツ記録方法および光ディスク

【特許請求の範囲】

【請求項１】　第１のディスク情報が記録されている第１情報領域と、個々のディスクを識別するための第２のディスク情報が記録されている第２情報領域と、光ビームを照射することにより情報の記録が可能なデータ領域を有することを特徴とする光ディスク。

【請求項２】　第２情報領域は、前記第１情報領域内に記録されていることを特徴とする請求項１記載の光ディスク。

【請求項３】　第２情報領域は、前記第１情報領域内の記録膜を、半径方向に長い形状でかつ複数個、部分的に除去することにより記録されていることを特徴とする請求項２記載の光ディスク。

【請求項４】　第１のディスク情報が記録されている第１情報領域と、個々のディスクを識別するための第２のディスク情報が記録されている第２情報領域と、光ビームを照射することにより情報の記録が可能なデータ領域を有する光ディスクの前記データ領域にコンテンツを記録する際に、少なくとも前記第２のディスク情報を用いた演算により、復号して再生することができるように暗号化して記録することを特徴とする暗号化コンテンツ記録方法。

【請求項５】　データ領域内に、暗号化されて記録されたデータを解読するための鍵情報を記録する鍵情報記録領域を有することを特徴とする請求項１記載の光ディスク。

【請求項６】　第１のディスク情報が記録されている第１情報領域と、個々のディスクを識別するための第２のディスク情報が記録されている第２情報領域と、光ビームを照射することにより情報の記録が可能なデータ領域と、前記データ領域内に、暗号化されて記録されたコンテンツを解読するための鍵情報を記録する鍵情報記録領域を有する光ディスクの、前記データ領域にコンテンツを記録する際に、少なくとも前記第２のディスク情報と、前記鍵情報を用いた演算により、復号して再生することができるように暗号化して記録することを特徴とする暗号化コンテンツ記録方法。

【請求項７】　第１のディスク情報は、微少な凹凸ピットにより構成されていることを特徴とする請求項１記載の光ディスク。

【請求項８】　第１のディスク情報は、微少な凹凸ピットにより構成されていることを特徴とする請求項４または６記載の暗号化コンテンツ記録方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、暗号化コンテンツ記録方法および書き換え型もしくは追記型の光ディスクに関する。

【０００２】

【従来の技術】

近年、再生専用光ディスク、特にＣＤ－ＲＯＭの普及に伴い、ＣＤ－ＲＯＭを用いたソフト流通システムが実用化されている。この場合ＣＤ－ＲＯＭを受け取ったユーザは、同梱のパスワードをパソコンから入力することにより、ＣＤ－ＲＯＭに予め記録されている暗号を解読する、もしくは暗号化されているコンテンツを解読するといった方法が一般的である。

【０００３】

しかしながらＣＤ－ＲＯＭの場合、ディスク上に追記記録できないため各ディスクのＩＤは個別に設定できない。従って１つのパスワードが全てのディスクの暗号を解読してしまうことになり、ディスクが不正にコピーされても、コンテンツの解読が可能であった。

【０００４】

この課題を解決するために、光ディスクのピット部にバーコードを重ね書きするための追記領域（以下ＢＣＡ領域と略す）を設け、光ディスク製造時にＢＣＡ領域にディスク毎に異なるＩＤを記録しておく方法が提案されている（国際公開番号ＷＯ９７／１４１４４）。

【０００５】

この方法によると、パスワードはディスクＩＤにより異なるので、１つのパスワードは１枚のディスクの暗号しか解読することができなくなり、コンテンツが

不正にコピーされてもディスクＩＤの情報が欠落しているため、コンテンツは解読されなくなる。

【０００６】

【発明が解決しようとする課題】

一方、インターネット等のネットワーク手段によりソフトを入手する場合には、再生専用光ディスクではなく、書き換え型の光ディスクを用いる方法が有望視されているが、書き換え型の光ディスクを用いたソフト流通システムの詳細については未だ確立されていない。

【０００７】

本発明は上記課題を鑑み、簡単なシステムで、ユーザ側の不正コピーを防止しつつ、ネットワークもしくは電波により発信されたコンテンツを光ディスクへ記録するための、暗号化コンテンツ記録方法を提供することを目的とする。

【０００８】

【課題を解決するための手段】

この課題を解決するために本発明の光ディスクは、第１のディスク情報が記録されている第１情報領域と、個々のディスクを識別するための第２のディスク情報が記録されている第２情報領域と、光ビームを照射することにより情報の記録が可能なデータ領域を有する。

【０００９】

また、この課題を解決するために本発明の光ディスクの第２情報領域は、前記第１情報領域内に記録されている。

【００１０】

また、この課題を解決するために本発明の光ディスクの第２情報領域は、前記第１情報領域内の記録膜を、半径方向に長い形状でかつ複数個、部分的に除去することにより記録されている。

【００１１】

また、この課題を解決するために本発明の暗号化コンテンツの記録方法は、第１のディスク情報が記録されている第１情報領域と、個々のディスクを識別するための第２のディスク情報が記録されている第２情報領域と、光ビームを照射す

ることにより情報の記録が可能なデータ領域を有する光ディスクの前記データ領域にコンテンツを記録する際に、少なくとも前記第２のディスク情報を用いた演算により、復号して再生することができるように暗号化して記録する。

【００１２】

また、この課題を解決するために本発明の光ディスクは、データ領域内に、暗号化されて記録されたデータを解読するための鍵情報を記録する鍵情報記録領域を有する。

【００１３】

また、この課題を解決するための本発明の暗号化コンテンツの記録方法は、第１のディスク情報が記録されている第１情報領域と、個々のディスクを識別するための第２のディスク情報が記録されている第２情報領域と、光ビームを照射することにより情報の記録が可能なデータ領域と、データ領域内に、暗号化されて記録されたコンテンツを解読するための鍵情報を記録する鍵情報記録領域を有する光ディスクの前記データ領域にコンテンツを記録する際に、少なくとも前記第２のディスク情報と、前記鍵情報を用いた演算により、復号して再生することができるように暗号化して記録する。

【００１４】

また、この課題を解決するための本発明の光ディスクは、第１のディスク情報が微少な凹凸ピットにより構成されている。

【００１５】

また、この課題を解決するための本発明の暗号化コンテンツの記録方法は、第１のディスク情報が微少な凹凸ピットにより構成されている。

【００１６】

【発明の実施の形態】

本発明の請求項１に記載の発明の光ディスクは、第１のディスク情報が記録されている第１情報領域と、個々のディスクを識別するための第２のディスク情報が記録されている第２情報領域と、光ビームを照射することにより情報の記録が可能なデータ領域を有するものであり、従来の光ディスクに、前記光ディスクを識別する情報を付加することにより、光ディスクの管理を容易に実現することが

できる。

【００１７】

本発明の請求項２に記載の発明によると、第２情報領域は、前記第１情報領域内に記録されているものであり、第１情報領域を再生する光ピックによって再生することができる。

【００１８】

本発明の請求項３に記載の発明によると、第２情報領域は、前記第１情報領域内の記録膜を、半径方向に長い形状でかつ複数個、部分的に除去することにより記録されているものであり、容易に前記第２情報が改ざんされることを防止することができる。

【００１９】

本発明の請求項４に記載の発明によると、暗号化コンテンツの記録方法は、第１のディスク情報が記録されている第１情報領域と、個々のディスクを識別するための第２のディスク情報が記録されている第２情報領域と、光ビームを照射することにより情報の記録が可能なデータ領域を有する光ディスクの前記データ領域にコンテンツを記録する際に、少なくとも前記第２のディスク情報を用いた演算により、復号して再生することができるように暗号化して記録するものであり、特定の１枚のディスクにしか存在しない光ディスク識別情報により暗号化することにより、コンテンツの不正なコピーを防止することができ、著作権が保護できるという効果がある。

【００２０】

本発明の請求項５に記載の発明の光ディスクは、データ領域内に、暗号化されて記録されたコンテンツを解読するための鍵情報を記録する鍵情報記録領域を有するものであり、暗号化されて記録されたコンテンツを解読する際に鍵情報が必要なシステムにおいて、鍵情報記録領域に鍵情報が一度記録されることにより、再生する度に鍵情報を入力する必要がなくなるという効果がある。

【００２１】

本発明の請求項６に記載の発明によると、暗号化コンテンツの記録方法は、第１のディスク情報が記録されている第１情報領域と、個々のディスクを識別する

ための第２のディスク情報が記録されている第２情報領域と、光ビームを照射することにより情報の記録が可能なデータ領域と、データ領域内に、暗号化されて記録されたコンテンツを解読するための鍵情報を記録する鍵情報記録領域を有する光ディスクの前記データ領域にコンテンツを記録する際に、少なくとも前記第２のディスク情報と、前記鍵情報を用いた演算により、復号して再生することができるように暗号化して記録するものであり、暗号化されたコンテンツを別の光ディスクにコピーされても、不正に再生されることはなく、暗号化されたコンテンツをコピーした光ディスクを再生する際には必ず課金が伴うことから著作権を保護することができる。

【００２２】

本発明の請求項７と８に記載の発明によると、第１のディスク情報は、微少な凹凸ピットにより構成されるものであり、ディスクを識別するための第２のディスク情報が、前記凹凸ピット上に記録されることにより、容易に第２のディスク情報が改ざんされることを防止することができる。

【００２３】

さらに第１のディスク情報と第２のディスク情報が隣接していることにより、第１の情報を再生する際に、第２の情報も続けて再生することができる、もしくは第２の情報を再生する際に、第１の情報を続けて再生することができるので、例えばディスクを起動する際にＣＰＵが速やかにディスクを識別するための第２の情報を入手し、暗号化されたコンテンツを記録するための処理を早めることが可能になる。

【００２４】

以下本発明の実施の形態における暗号化コンテンツ記録再生方法について図面を参照しながら説明する。

【００２５】

（実施の形態１）

図１は本発明による第１の実施の形態の光ディスクの平面図である。

【００２６】

図１において１０１は書き換え型もしくは追記型の光ディスク（以下光ディス

ク）、１０２はディスク情報を凹凸ピットで記録してあるコントロールデータ領域、１０３はユーザがデータを記録するデータ領域、１０４はディスクＩＤを記録してあるＢＣＡ領域である。

【００２７】

ＢＣＡ領域１０４では、コントロールデータ領域１０２の内周部分の凹凸ピット上の記録膜が、１０５の様に半径方向に長い形状でかつ複数個、部分的にＹＡＧレーザなどのパルスレーザでトリミングされている。

【００２８】

図２はＢＣＡ領域１０４を再生したときの出力信号の説明図である。また図３はＢＣＡ領域１０４を再生する回路であり、３０１は光ピック、３０２はプリアンプ、３０３はローパスフィルタ、３０４は二値化回路、３０５は復調回路である。

【００２９】

光ピック３０１から出力されるレーザ光は光ディスク１０１のＢＣＡ領域１０４を照射し、その反射光がプリアンプ３０２で増幅されて信号２０１が得られる。

【００３０】

信号２０１はコントロールデータ領域１０２の凹凸ピットによる信号であるが、２０２、２０３、２０４はパルスレーザによるトリミングで、記録膜が取り除かれて、凹凸ピットによる信号が欠落している部分である。なおトリミングはディスク製造者によって行われる。

【００３１】

信号２０１はローパスフィルタ３０３に入力されて、凹凸ピットによる変調信号が除去された後に、二値化回路３０４に入力され、通常コントロールデータ領域の信号を二値化するスライスレベル２０５ではなく、スライスレベル２０６によって二値化されて信号２０７が得られる。二値化回路３０４の出力信号は、復調回路３０５で復調されてディスクＩＤ信号３０６が得られる。

【００３２】

以上の様に、光ディスクを識別する情報を付加することにより、光ディスクの

管理を容易に実現することができる。またＢＣＡ領域が凹凸ピット上に記録されることにより、ＢＣＡ領域内の光ディスクを識別する情報が容易に改ざんされることを防止することができる。

【００３３】

さらにコントロールデータ領域１０２とＢＣＡ領域１０４が隣接していることにより、コントロールデータ領域１０２を再生する際に、ＢＣＡ領域１０４も続けて再生することができる、もしくはＢＣＡ領域１０４を再生する際に、コントロールデータ領域１０２を続けて再生することができるので、例えばディスクを起動する際にＣＰＵが速やかにディスクを識別するためのＢＣＡ領域１０４の情報を入手し、暗号化されたコンテンツを記録するための処理を早めることが可能になる。

【００３４】

なお本実施の形態のＢＣＡ領域１０４は、コントロールデータ領域１０２の内周部分の凹凸ピット上の記録膜をトリミングしているが、書き換え型もしくは追記型の光ディスクを構成する記録膜は、再生専用の光ディスクにおける反射膜に対して熱による影響を受けやすい。コントロールデータ領域１０２の内周部分をトリミングすることにより、外周部分をトリミングする場合に比べて、トリミングの際に発生する熱からデータ領域１０３を保護することができる。

【００３５】

なおトリミング前のＢＣＡ領域１０４に記録されているデータが、コントロールデータ領域１０２に記録されていても良い。ＢＣＡ領域１０４に記録されているデータが、コントロールデータ領域１０２にも記録されていることにより、トリミングを行ってもコントロールデータ領域１０２の前記データを保護することができる。

【００３６】

さらに前記データがＢＣＡ領域１０４から、コントロールデータ領域１０２まで連続して繰り返し記録されている場合には、コントロールデータ領域１０２の前記データを見つけることによって、ＢＣＡ領域１０４の位置を予想することができる。

【００３７】

次に、以上の様なＢＣＡ領域を有する光ディスクに、ネットワークを通して、ディスクＩＤで暗号化されたコンテンツを記録する手順を述べる。図４はＢＣＡ領域を有する書き換え型もしくは追記型の光ディスクを用いて暗号化コンテンツを記録する際のブロック図である。

【００３８】

図４において、１０１は光ディスク、３０１は光ピック、４０１はＢＣＡ再生部、４０２はディスクＩＤ信号、４０３、４０４はインターフェース、４０５はネットワーク、４０６は暗号化部、４０７は映像ソフト等のコンテンツ、４０８は暗号化エンコーダ、４０９は暗号化コンテンツ、４１０は記録再生装置、４１１は記録回路、４１２はデータ再生部、４１３は暗号デコーダである。

【００３９】

まず、光ピック３０１から出力されるレーザ光がＲＡＭディスク１０１のＢＣＡ領域１０４を照射し、その反射光がＢＣＡ再生部４０１に入力され、ＢＣＡ再生部４０１はディスクＩＤ信号４０２を出力し、インターフェース４０３、４０４とネットワーク４０５を介して、暗号化部４０６に送られる。

【００４０】

暗号化部４０６では、コンテンツ４０７が記録される光ディスク１０１のディスクＩＤ信号４０２が暗号を解く復号鍵となるように、暗号化エンコーダ４０８において暗号化もしくは映像音声用のスクランブルを行う。

【００４１】

なお本実施の形態では、暗号化処理について、コンテンツ４０７をディスクＩＤ信号４０２を暗号鍵として暗号化すると表現しても同意とする。

【００４２】

また本実施の形態においては、暗号化や復号化を錠と鍵の関係で考え、前記錠を前記鍵で閉めることを暗号化とし、前記錠を前記鍵で開けることを復号化とする。従って暗号化と復号化で実際の演算は異なるが、暗号化するための鍵と復号化するための鍵は、同一であるとする。

【００４３】

なおコンテンツ４０７をC、ディスクＩＤ信号４０２をＢＣＡ、暗号化されたコンテンツ４０９をＣ［ＢＣＡ］、暗号化処理を＊すると、Ｃ＊ＢＣＡ＝Ｃ［ＢＣＡ］と表記する。

【００４４】

暗号化されたコンテンツ４０９は、インターフェース４０３、４０４とネットワーク４０５を介して記録再生装置４１０に送られ、記録回路４１１の出力信号に応じて光ピック３０１により光ディスク１０１に記録される。

【００４５】

次に、光ディスク１０１に暗号化されて記録された前記コンテンツを再生する際は、光ピック３０１から出力されるレーザ光がデータ領域１０３の前記暗号化コンテンツが記録された領域を照射し、その反射光がデータ再生部４１２に入力され、データ再生部４１２の出力信号は暗号デコーダ４１３に入力される。

【００４６】

一方で、光ピック３０１から出力されるレーザ光は光ディスク１０１のＢＣＡ領域１０４を照射し、その反射光がＢＣＡ再生部４０１に入力され、ＢＣＡ再生部４０１はディスクＩＤ信号４０２を出力し、出力信号は暗号デコーダ４１３に入力される。

【００４７】

暗号デコーダ４１３では、入力されたディスクＩＤ信号４０２を鍵として、暗号化された信号の復号を行う。このときコンテンツが正規に光ディスク１０１に記録されている場合は、光ディスク１０１に記録されている暗号化コンテンツを復号するための鍵は、光ディスク１０１のディスクＩＤ信号であり、再生時にＢＣＡ再生部から出力されるディスクＩＤ信号も、光ディスク１０１のディスクＩＤ信号であるので、復号もしくはデスクランブルされたコンテンツが、暗号デコーダ４１３から出力される。なお復号化処理を＃すると、Ｃ［ＢＣＡ］＃ＢＣＡ＝Ｃと表記される。コンテンツが映像情報の場合は例えばＭＰＥＧ信号が伸長されて、映像信号が得られる。

【００４８】

以上の様に、本実施の形態における暗号化は、ディスクＩＤを鍵としており、

ディスクＩＤは世の中に１枚しか存在しないため、１枚の光ディスクにしか同じ暗号化コンテンツの記録ができないという効果がある。

【００４９】

前記コンテンツ４０７を、例えばＩＤ１というディスクＩＤを持つ正規の光ディスクから、ＩＤ２という別のディスクＩＤを持つ別の光ディスクにコピーして再生しようとした場合、ＢＣＡ再生部４０１からディスクＩＤ信号４０２としてＩＤ２が出力される。しかし暗号化コンテンツはＩＤ１というディスクＩＤ信号で暗号化されているので、暗号デコーダ４１３で、暗号化コンテンツを復号することができない。

【００５０】

なお、暗号化エンコーダ４０８はコンテンツの供給元ではなく、ネットワークに対して記録再生装置側にあり、暗号化エンコーダを搭載したＩＣカード等の形態であっても良い。

【００５１】

また、前記光ディスク１０１はディスクＩＤのみで暗号化されているので、ＢＣＡ再生部と暗号デコーダを有する任意の光ディスク記録再生装置で再生することが可能である。

【００５２】

以下本発明の異なる実施の形態における暗号化コンテンツ記録方法について図面を参照しながら説明する。

【００５３】

（実施の形態２）

図５は本発明による第２の実施の形態における、ＢＣＡ領域を有する書き換え型もしくは追記型の光ディスクを用いて暗号化コンテンツを記録する際のブロック図である。なお、第１の実施の形態と共通の部分は説明を簡略化する。

【００５４】

図５において、５０１はＣＡＴＶ会社、５０２は映画ソフト等のコンテンツ、５０３は第１暗号鍵、５０４は第１暗号化エンコーダ、５０５は第１暗号化コンテンツ、５０６はＣＡＴＶデコーダ、５０７は鍵発行センター、５０８はＣＡＴ

Ｖデコーダ５０６のシステムＩＤ、５０９はコンテンツ５０２のタイトルコード、５１０は時間制限情報、５１１は記録許可コード、５１３は第１暗号デコーダ、１０１はＢＣＡ領域を有する書き換え型もしくは追記型の光ディスク（以下光ディスク）、５１４は光ディスク記録装置、５１５は光ディスク１０１のディスクＩＤ信号、５１６は第２暗号化エンコーダ、５１７は第２暗号化コンテンツ、５１８は記録回路、５１９はデータ再生部、５２０は第２暗号デコーダ、５２１はＢＣＡ再生部、５２２、５２４はＩＣカード、５２３、５２６は会社識別信号である。

【００５５】

まずＣＡＴＶ会社５０１は、映画ソフト等のコンテンツ５０２を第１暗号鍵５０３を用いて第１暗号化エンコーダ５０４にて暗号化し、第１暗号化コンテンツ５０５を生成し、ネットワークを介して各ユーザのＣＡＴＶデコーダ５０６に送信する。

【００５６】

ここでコンテンツ５０２をＣ、第１暗号鍵５０３をＦＫ、第１暗号化コンテンツ５０５をＣ［ＦＫ］とすると、Ｃ＊ＦＫ＝Ｃ［ＦＫ］と表記される。

【００５７】

ＣＡＴＶデコーダ５０６は、ネットワークを介して鍵発行センター５０７へ、ＣＡＴＶデコーダ５０６のシステムＩＤ５０８と、視聴もしくはＲＡＭディスクへの記録を行いたい前記コンテンツのタイトルコード５０９を送る。

【００５８】

なお、タイトルコード５０９はＴＶの画面に従って選択することにより入力しても良いし、直接キーボードから入力しても良いし、リモートコントローラー等から入力しても良い。従ってタイトルコード５０９は、ユーザが独自に入手していても良いし、第１暗号化コンテンツ５０５と共にＣＡＴＶデコーダ５０６に送られてきても良いし、番組案内等の形態で第１暗号化コンテンツ５０５とは別の時間に予め送られていても良い。

【００５９】

鍵発行センター５０７は、ＣＡＴＶデコーダ５０６のシステムＩＤ５０８、前

記コンテンツのタイトルコード５０９、時間制限情報５１０、記録許可コード５１１に対応する鍵Ｋ５１２を記録許可コード５１１と共にＣＡＴＶデコーダ５０６の第１暗号デコーダ５１３へネットワークを介して送信する。

【００６０】

なお時間制限情報５１０により、同一のコンテンツを時間を変えて複数回放送する場合を区別することができる。

【００６１】

ここで第１復号鍵をＦＫ、ＣＡＴＶデコーダ５０６のシステムＩＤ５０８をＤＩＤ、時間制限情報５１０をＴＩＭＥ、記録許可コード５１１をＣＯＰＹ、コンテンツのタイトルコード５０９をＴとするとき鍵Ｋは、ＦＫ＝Ｋ＊Ｔ＊ＤＩＤ＊ＴＩＭＥ＊ＣＯＰＹの関係を満たしている。

【００６２】

なお記録許可コード５１１は、例えばＣＡＴＶ会社５０１が、放送するコンテンツが新作品か旧作品かを判断して、視聴のみ許可するのか、視聴、記録の両方を許可するのかを決定する。

【００６３】

第１暗号デコーダ５１３は鍵Ｋ５１２と、前記コンテンツ５０２のタイトルコード５０９と、システムＩＤ５０８と、記録許可コード５１１に加えて、時間情報５２７が時間制限情報５１０の条件を満たしていれば、第１暗号化コンテンツ５０５を復号し、映像信号の場合は、デスクランブルされた信号が出力され、ＴＶで視聴できる。

【００６４】

ここで復号化処理を式で表すと、Ｃ［ＦＫ］＃（Ｋ＊Ｔ＊ＤＩＤ＊ＴＩＭＥ＊ＣＯＰＹ）＝Ｃ［ＦＫ］＃ＦＫ＝Ｃとなる。

【００６５】

なお、記録許可コード５１１が視聴のみ許可する場合は、光ディスク１０１に記録できないが、視聴、記録の両方を許可する場合は記録することができるので、以降でこの方法について説明する。

【００６６】

光ディスク記録装置５１４は、光ディスク１０１のＢＣＡ領域１０４を再生し、ディスクＩＤ信号５１５がＢＣＡ再生部５２１の出力信号としてＣＡＴＶデコーダ５０６の第２暗号化エンコーダ５１６に送られる。

【００６７】

第２暗号化エンコーダ５１６ではディスクＩＤ信号５１５を第２暗号鍵として用いて、第１暗号デコーダ５１３から出力されたコンテンツを第２暗号化エンコーダにて暗号化し、第２暗号化コンテンツ５１７を生成し、光ディスク記録装置に送信する。

【００６８】

なお前記暗号化は第１暗号デコーダ５１３から第１暗号化コンテンツが復号されて出力されている間に限られる。

【００６９】

ここで、第１暗号デコーダ５１３の出力信号であるコンテンツをＣ、第２暗号鍵であるディスクＩＤ信号５１５をＢＣＡ、第２暗号化コンテンツ５１７をＣ［ＢＣＡ］とするとするとき、Ｃ＊ＢＣＡ＝Ｃ［ＢＣＡ］と表記される。

【００７０】

光ディスク記録装置５１４に送られた第２暗号化コンテンツ５１７は、記録回路５１８により例えば８－１６変調により変調されて、図示しない光ピックにより光ディスク１０１のデータ領域１０３に記録される。

【００７１】

光ディスク１０１に暗号化されて記録された前記コンテンツを再生する際は、光ピックから出力されるレーザ光が光ディスク１０１の前記暗号化されたコンテンツが記録されている領域を照射し、その反射光がデータ再生部５１９に入力され、データ再生部５１９の出力信号は第２暗号デコーダ５２０に入力される。

【００７２】

一方で、光ピックから出力されるレーザ光は光ディスク１０１のＢＣＡ領域１０４を照射し、その反射光がＢＣＡ再生部５２１に入力され、ＢＣＡ再生部５２１はディスクＩＤ信号５１５を出力し、出力信号は第２暗号デコーダ５２０に入力される。

【００７３】

第２暗号デコーダ５２０では、入力されたディスクＩＤ信号５１５を鍵として、暗号化されたコンテンツの復号を行う。このときコンテンツが正規に光ディスク１０１に記録されている場合は、光ディスク１０１に記録されている暗号化コンテンツを復号するための鍵は光ディスク１０１のディスクＩＤであり、ＢＣＡ再生部５１４から出力されるディスクＩＤ信号も、光ディスク１０１のディスクＩＤ信号であるので、復号もしくはデスクランブルされたコンテンツが、第２暗号デコーダ５２０から出力される。

【００７４】

ここで復号化処理を式で記述すると、Ｃ［ＢＣＡ］＃ＢＣＡ＝Ｃとなる。コンテンツが映像情報の場合は例えばＭＰＥＧ信号が伸長されて、映像信号が得られる。

【００７５】

また、前記光ディスク１０１はディスクＩＤ５１５のみで暗号化されているので、ＢＣＡ再生部と第２暗号デコーダを有する任意の光ディスク記録装置で再生することが可能である。

【００７６】

なお、暗号エンコーダで暗号化、暗号デコーダで複合化を説明したが、ＣＰＵの中のプログラムである暗号アルゴリズムおよび復号アルゴリズムを用いても良い。

【００７７】

なお本実施の形態では、第２暗号化エンコーダ５１６ではディスクＩＤ信号５１５を第２暗号鍵として用いて暗号化したが、例えば各ＣＡＴＶ会社毎に準備されたＩＣカード５２２をＣＡＴＶデコーダ５０６に装着して、ＩＣカード内に記録されている会社識別信号５２３とディスクＩＤ信号５１５を組み合わせて第２暗号鍵とし、第２暗号化エンコーダ５１６にて暗号化しても良い。

【００７８】

ここで、第１暗号デコーダ５１３の出力信号であるコンテンツをＣ、第１の第２暗号鍵であるディスクＩＤ５１５をＢＣＡ、第２の第２暗号鍵である会社識別

信号５２３をＣＫ、第２暗号化コンテンツ５１７をＣ［ＢＣＡ，ＣＫ］とするとき、暗号化処理を式で記述すると、Ｃ＊ＢＣＡ＊ＣＫ＝Ｃ［ＢＣＡ，ＣＫ］と表記される。

【００７９】

次に光ディスク１０１に暗号化して記録されたコンテンツを再生する際には、光ピックから出力されるレーザ光が光ディスク１０１の前記暗号化されたコンテンツが記録されている領域を照射し、その反射光がデータ再生部５１９に入力され、データ再生部５１９の出力信号は第２暗号デコーダ５２０に入力される。

【００８０】

一方で、光ピックから出力されるレーザ光は光ディスク１０１のＢＣＡ領域１０４を照射し、その反射光がＢＣＡ再生部５２１に入力され、ＢＣＡ再生部５２１はディスクＩＤ信号５１５を出力し、出力信号は第２暗号デコーダ５２０に入力される。

【００８１】

さらに光ディスク記録装置５１４に装着されたＩＣカード５２４内の会社識別信号５２６が第２暗号デコーダ５２０に入力される。なお会社識別信号５２６は、ＩＣカード５２４内に記録されていなくても良く、インストールによって光ディスク記録装置５１４内のメモリに記録されていても良いし、ＩＣカード５２２内の会社識別信号５２３が入力されても良い。

【００８２】

第２暗号デコーダ５２０では、入力されたディスクＩＤ信号５１５と会社識別信号５２６を復号鍵として、暗号化された信号の復号を行う。このとき特定のＣＡＴＶ会社５０１と正式に契約をし、コンテンツ５０２が正規に光ディスク１０１に記録されている場合は、光ディスク１０１に暗号化されて記録されている暗号化コンテンツの第１の復号鍵は、まさに再生しようとする光ディスク１０１のディスクＩＤ信号であり、第２の復号鍵は、契約したＣＡＴＶ会社５０１から提供されたＩＣカード５２４内の会社識別信号５２６であるので、復号もしくはデスクランブルされたコンテンツ５２５が、第２暗号デコーダ５２０から出力される。

【００８３】

復号化処理を式で記述すると、Ｃ［ＢＣＡ，ＣＫ］＃（ＢＣＡ＊ＣＫ）＝Ｃとなる。コンテンツ５２５が映像情報の場合は例えばＭＰＥＧ信号が伸長されて、映像信号が得られる。

【００８４】

また、前記光ディスク１０１はディスクＩＤ５１５と会社識別信号５２１で暗号化されているので、前記コンテンツの提供元のＣＡＴＶ会社と契約を結んでいれば、ＢＣＡ再生部と、第２暗号デコーダを有する任意の光ディスク記録再生装置で再生することが可能である。

【００８５】

逆に前記ＣＡＴＶ会社５０１と契約していなければ、会社識別信号を入手できないので、コンテンツを再生することができず、契約済みのユーザとの差別化を可能にする。

【００８６】

また本実施の形態では、各ユーザは自宅のＣＡＴＶデコーダに光ディスク記録装置からディスクＩＤ信号を送り、画像データ等を暗号化するので、ＣＡＴＶ会社は各ユーザに配信する暗号化コンテンツを個別に変える必要がなく、放送時のシステムを簡単にでき、低コストで、大量の視聴者に同じコンテンツを提供することができる。さらに本実施の形態によるとＣＡＴＶデコーダを有する各ユーザ毎にＲＡＭディスク１枚だけに記録を許可することができる。

【００８７】

なお本実施の形態ではケーブルテレビからのコンテンツを放送する場合について説明したが、電波による放送でも同様である。

【００８８】

以下本発明の異なる実施の形態における暗号化コンテンツ記録再生方法について図面を参照しながら説明する。図６は本発明による第３の実施の形態における、ＢＣＡ領域を有する書き換え型もしくは追記型の光ディスクである。

【００８９】

また図７は図６の光ディスクを用いて暗号化コンテンツを記録する際のブロッ

ク図である。なお、第１、第２の実施の形態と共通の部分は説明を簡略化する。

【００９０】

図６において、６０１は書き換え型もしくは追記型の光ディスク（以下光ディスク）、６０２はディスク情報を凹凸ピットで記録してあるコントロールデータ領域、６０３はユーザがデータを記録するデータ領域、６０４はディスクＩＤを記録してあるＢＣＡ領域である。

【００９１】

ＢＣＡ領域６０４では、コントロールデータ領域１０２の内周部分の凹凸ピット上の記録膜が、６０６の様に半径方向に長い形状でかつ複数個、部分的にＹＡＧレーザなどのパルスレーザでトリミングされている。

【００９２】

なおトリミングはディスク製造者によって行われる。またディスクＩＤを付加することにより、光ディスクの管理を容易に実現することができる。さらにＢＣＡ領域が凹凸ピット上に記録されることにより、ＢＣＡ領域内の光ディスクを識別する情報が容易に改ざんされることを防止することができる。

【００９３】

さらにコントロールデータ領域６０２とＢＣＡ領域６０４が隣接していることにより、コントロールデータ領域６０２を再生する際に、ＢＣＡ領域６０４も続けて再生することができる、もしくはＢＣＡ領域６０４を再生する際に、コントロールデータ領域６０２を続けて再生することができるので、例えば光ディスクを起動する際にＣＰＵが速やかにディスクを識別するためのＢＣＡ領域６０４の情報を入手し、暗号化されたコンテンツを記録するための処理を早めることが可能になる。

【００９４】

なお本実施の形態のＢＣＡ領域６０４は、コントロールデータ領域６０２の内周部分の凹凸ピット上の記録膜をトリミングしているが、書き換え型もしくは追記型の光ディスクを構成する記録膜は、再生専用の光ディスクにおける反射膜に対して熱による影響を受けやすい。コントロールデータ領域６０２の内周部分をトリミングすることにより、外周部分をトリミングする場合に比べて、トリミン

グの際に発生する熱からデータ領域６０３を保護することができる。

【００９５】

なおトリミング前のＢＣＡ領域６０４に記録されているデータが、コントロールデータ領域６０２に記録されていても良い。ＢＣＡ領域６０４に記録されているデータが、コントロールデータ領域６０２にも記録されていることにより、トリミングを行ってもコントロールデータ領域６０２の前記データを保護することができる。

【００９６】

さらに前記データがＢＣＡ領域６０４から、コントロールデータ領域６０２まで連続して繰り返し記録されている場合には、コントロールデータ領域６０２の前記データを見つけることによって、ＢＣＡ領域６０４の位置を予想することができる。

【００９７】

また６０５は鍵情報記録領域である。鍵情報記録領域６０５は、データ領域６０３と同じく光ビームを照射することにより記録される。

【００９８】

本実施の形態のように、コントロールデータ領域６０２と鍵情報記録領域６０５が隣接していることにより、コントロールデータ領域６０２を再生する際に、鍵情報記録領域６０５も続けて再生することができる、もしくは鍵情報記録領域６０５を再生する際に、コントロールデータ領域６０２を続けて再生することができるので、例えば光ディスクを起動する際にＣＰＵが速やかにディスクを識別するためのＢＣＡ領域６０４の情報を入手し、暗号化されたコンテンツを再生するための処理を早めることが可能になる。

【００９９】

図７において、７０１はＣＡＴＶ会社、７０２は映画ソフト等のコンテンツ、７０３は第１暗号鍵、７０４は第１暗号化エンコーダ、７０５は第１暗号化コンテンツ、７０６はＣＡＴＶデコーダ、７０７は鍵発行センター、７０８はＣＡＴＶデコーダ７０６のシステムＩＤ、７０９はコンテンツ７０２のタイトルコード、７１０は時間制限情報、７１３は第１暗号デコーダ、７１４は光ディスク記録

装置、７１５は光ディスク６０１のディスクＩＤ、７１６はコンテンツ７０２のタイトルコード、７１７は記録回路、７１９は鍵情報記録回路、７２０はＢＣＡ再生部、７２１はデータ再生部、７２２は第２暗号デコーダ、７２３は鍵情報再生部である。

【０１００】

まずＣＡＴＶ会社７０１は、映画ソフト等のコンテンツ７０２を第１暗号鍵７０３を用いて第１暗号化エンコーダ７０４にて暗号化し、第１暗号化コンテンツ７０５を生成し、各ユーザのＣＡＴＶデコーダ７０６に送信する。

【０１０１】

ここでコンテンツ７０２をＣ、第１暗号鍵７０３をＦＫ、第１暗号化コンテンツ７０５をＣ［ＦＫ］とすると、Ｃ＊ＦＫ＝Ｃ［ＦＫ］と表記される。

【０１０２】

ＣＡＴＶデコーダ７０６はネットワークを介して鍵発行センター７０７へ、ＣＡＴＶデコーダ７０６のシステムＩＤ７０８と、視聴したい前記コンテンツのタイトルコード７０９を送る。

【０１０３】

なお、タイトルコード７０９はＴＶの画面に従って選択することにより入力しても良いし、直接キーボードから入力しても良いし、リモートコントローラー等から入力しても良い。従ってタイトルコード７０９は、ユーザが独自に入手していても良いし、第１暗号化コンテンツ７０５と共にＣＡＴＶデコーダ７０６に送られてきても良いし、番組案内等の形態で第１暗号化コンテンツ７０５とは別の時間に予め送られていても良い。

【０１０４】

鍵発行センター７０７は、ＣＡＴＶデコーダ７０６のシステムＩＤ７０８、前記コンテンツのタイトルコード７０９、時間制限情報７１０に対応する鍵Ｋ７１２をＣＡＴＶデコーダ７０６の第１暗号デコーダ７１３へネットワークを介して送信する。

【０１０５】

なお時間制限情報７１０により、同一のコンテンツを時間を変えて複数回放送

する場合を区別することができる。

【０１０６】

ここで第１復号鍵をＦＫ、ＣＡＴＶデコーダ７０６のシステムＩＤ７０８をＤＩＤ、時間制限情報７１０をＴＩＭＥ、コンテンツのタイトルコード７０９をＴとするとき、鍵Ｋは、ＦＫ＝Ｋ＊Ｔ＊ＤＩＤ＊ＴＩＭＥの関係を満たしている。

【０１０７】

第１暗号デコーダ７１３は鍵Ｋ７１２と、前記コンテンツのタイトルコード７０９と、システムＩＤ７０８に加えて、時間情報７２５が時間制限情報７１０の条件を満たしていれば、第１暗号化コンテンツ７０５を復号し、映像信号の場合は、デスクランブルされた信号が出力され、ＴＶで視聴できる。復号化処理を式で表すと、Ｃ［ＦＫ］＃（Ｋ＊Ｔ＊ＤＩＤ＊ＴＩＭＥ）＝Ｃ［ＦＫ］＃ＦＫ＝Ｃとなる。

【０１０８】

次に前記コンテンツを光ディスク６０１に記録する方法を説明する。光ディスク６０１へ記録する際には、ＣＡＴＶデコーダ７０６にて復号化されていない、第１暗号化コンテンツ７０５が光ディスク記録装置７１４に送られ、記録回路７１７により例えば８－１６変調により変調されて、図示されていない光ピックにより光ディスク６０１に記録される。

【０１０９】

従って光ディスク６０１に暗号化されて記録された前記コンテンツを再生するためには、第１暗号化コンテンツ７０５を復号する必要がある。

【０１１０】

光ディスク記録装置７１４はネットワークを介して鍵発行センター７０７へ、光ディスク６０１のディスクＩＤ７１５と、再生したい前記コンテンツのタイトルコード７１６を送る。

【０１１１】

なおディスクＩＤ７１５を送るタイミングは、鍵発行センター７０７とアクセスする際に送っても良いし、視聴の際に、タイトルコードと一緒に送っても良い。

【０１１２】

またディスクＩＤの送信方法も、図７に示すように光ディスク６０１のＢＣＡ領域６０４を再生して、ＢＣＡ再生部７２０の出力信号を直接鍵発行センター７０７に送る以外にも、例えばディスク起動時等の、鍵発行センター７０７とのアクセス以前にＢＣＡ領域６０４を再生して、光ディスク記録装置７１４やＣＡＴＶデコーダ７０６に保管しておき前記タイミングで鍵発行センター７０７に送っても良い。

【０１１３】

さらにディスクＩＤが、ラベル等の形態で視覚的にも認識できる場合には、キーボードから入力しても良いし、ラベルがバーコードになっている場合にはバーコードリーダーから読みとっても良い。

【０１１４】

鍵発行センター７０７は、光ディスク６０１のディスクＩＤ７１５、コンテンツのタイトルコード７１６に対応する鍵ＤＫ７１８を、光ディスク記録装置７１４の暗号記録回路７１９へ送信する。

【０１１５】

ここで第１復号鍵をＦＫ、光ディスク６０１のディスクＩＤ７１５をＢＣＡ、コンテンツのタイトルコード７１６をＴとするとき、鍵ＤＫは、ＦＫ＝ＤＫ＊ＢＣＡ＊Ｔの関係を満たしている。

【０１１６】

光ディスク記録装置７１４の鍵情報記録回路７１９に入力された鍵ＤＫは、例えば８－１６変調により変調されて、光ピックにより光ディスク６０１の鍵情報記録領域６０５に記録される。

【０１１７】

なお鍵ＤＫは鍵情報記録領域６０５に、同じ鍵が複数個記録されても良い。同じ鍵が複数個記録されることにより、鍵情報記録領域６０５の記録膜が劣化した場合や、傷がついた場合に鍵ＤＫを保護することができる。

【０１１８】

また本実施の形態では、鍵情報記録領域６０５はデータ領域６０３の内周側に

設けられているが、データ領域６０３の外周側にあっても良く、内周側と外周側の両方に設けられていても良い。外周側に設けられることにより、より多くの鍵ＤＫを記録することが可能となる。また鍵情報記録領域が複数個、分散して設けられることにより、一つの鍵情報記録領域が再生できなくなった場合でも、他の鍵情報記録領域により鍵ＤＫを保護することができる。

【０１１９】

一方、光ピックから出力されるレーザ光が光ディスク６０１の前記コンテンツが記録された領域を照射し、その反射光がデータ再生部７２１に入力され、データ再生部７２１は暗号化された信号を出力し、出力信号は第２暗号デコーダ７２２に入力される。

【０１２０】

さらに光ピックから出力されるレーザ光は光ディスク６０１のＢＣＡ領域６０４を照射し、その反射光がＢＣＡ再生部７２０に入力され、ＢＣＡ再生部７２０はディスクＩＤ信号７１５を出力し、出力信号は暗号デコーダ７２２に入力される。

【０１２１】

さらに、光ピックから出力されるレーザ光は光ディスク６０１の鍵情報記録領域６０５を照射し、その反射光が鍵情報再生部７２３に入力され、鍵情報再生部は鍵ＤＫを出力し、出力信号は第２暗号デコーダ７２２に入力される。

【０１２２】

なお、鍵発行センター７０７とアクセスしてすぐに再生する際は、鍵情報記録回路７１９は、鍵ＤＫを鍵情報記録領域６０５に記録する前に、直接第２暗号デコーダに入力しても良い。この様にすることにより、再生を開始するまでの時間を短縮することができる。

【０１２３】

暗号デコーダ７２２では、入力されたディスクＩＤ信号７１５と、鍵ＤＫと、前記コンテンツのタイトルコード７１６からなる復号鍵により、暗号化された信号の復号を行う。復号化処理を式で表すと、Ｃ［ＦＫ］＃（ＤＫ＊ＢＣＡ＊Ｔ）＝Ｃ［ＦＫ］＃ＦＫ＝Ｃとなる。コンテンツが映像情報の場合は例えばＭＰＥＧ

信号が伸長されて、映像信号が得られる。

【０１２４】

鍵発行センター７０７から鍵信号を受け取るときに課金されるとすると、本実施の形態によると、視聴するときと、光ディスク６０１に記録したコンテンツを初めて再生するときに別々に課金され、光ディスク６０１に記録しただけでは課金されない。

【０１２５】

従って、視聴と光ディスク６０１への記録の両方に対してまとめて課金する場合に対して、視聴はしたいが光ディスク６０１に記録する必要がないユーザや、光ディスク６０１に記録したいが、放送されるときに視聴する必要がないユーザにとっては課金される金額を安くすることができる。

【０１２６】

また光ディスク６０１に記録しただけでは課金されないので、ユーザは視聴した後で、再度視聴するために光ディスク６０１を再生するための鍵を受け取るかどうかを決定することができる。

【０１２７】

なお、鍵ＤＫは鍵発行センター７０７からネットワークにより受け取る以外にも、コンテンツのタイトルとディスクＩＤ番号を電話等で口頭で伝えることにより、口頭で受け取ってキーボードから入力しても良い。

【０１２８】

次に、鍵情報記録領域６０５に鍵ＤＫが記録された光ディスク６０１を鍵発行センター７０７とのアクセス終了後に再生する場合について説明する。

【０１２９】

まず、光ピックから出力されるレーザ光が光ディスク６０１の前記コンテンツが記録された領域を照射し、その反射光がデータ再生部７２１に入力され、データ再生部７２１は暗号化された信号を出力し、出力信号は第２暗号デコーダ７２２に入力される。

【０１３０】

一方、光ピックから出力されるレーザ光は光ディスク６０１のＢＣＡ領域６０

４を照射し、その反射光がＢＣＡ再生部７２０に入力され、ＢＣＡ再生部７２０はディスクＩＤ信号７１５を出力し、出力信号は第２暗号デコーダ７２２に入力される。

【０１３１】

さらに、光ピックから出力されるレーザ光は光ディスク６０１の鍵情報記録領域６０５を照射し、その反射光が鍵情報再生部７２３に入力され、鍵情報再生部は鍵ＤＫを出力し、出力信号は第２暗号デコーダ７２２に入力される。

【０１３２】

第２暗号デコーダ７２２では、入力されたディスクＩＤ信号７１５と、鍵ＤＫと、前記コンテンツのタイトルコード７１６からなる復号鍵により、暗号化されたコンテンツの復号を行う。復号化処理を式で表すと、Ｃ［ＦＫ］＃（ＤＫ＊ＢＣＡ＊Ｔ）＝Ｃ［ＦＫ］＃ＦＫ＝Ｃとなる。コンテンツが映像情報の場合は例えばＭＰＥＧ信号が伸長されて、映像信号が得られる。

【０１３３】

鍵情報記録領域６０５に鍵ＤＫが一度記録されることにより、鍵発行センター７０７とのアクセスをすることなく、いつでも前記暗号化コンテンツを再生することができる。

【０１３４】

また、復号化処理に必要な復号鍵は全て光ディスク６０１に記録されているので、前記光ディスク６０１は、ＢＣＡ再生部、鍵情報再生部、第２暗号デコーダを有する任意の光ディスク記録装置で再生することができる。

【０１３５】

また前記暗号化コンテンツをディスクＩＤの異なる光ディスクにコピーして再生しようとした場合には、ＢＣＡ再生部から前記光ディスク６０１とは異なるディスクＩＤ信号が出力されるので、暗号化されたコンテンツを復号することができず、コンテンツはコピーされても再生されない。

【０１３６】

ただこの場合にも、コンテンツのタイトルとディスクＩＤをネットワークもしくは口頭で鍵発行センターに伝えることにより、課金の後、復号鍵を受け取って

も良い。このように、暗号化されたコンテンツを別の光ディスクにコピーされても、不正に再生されることはなく、暗号化されたコンテンツをコピーした光ディスクを再生する際には必ず課金が伴うことから著作権を保護することができる。

【０１３７】

図８にシステムＩＤ、ディスクＩＤが異なる場合の第１暗号デコーダ７１３に入力される鍵Ｋ、鍵情報記録回路７１９に入力される鍵ＤＫを整理する。図８において、Ｔ１、Ｔ２、Ｔ３は異なるコンテンツのタイトルコード、ＦＫ１、ＦＫ２、ＦＫ３はそれぞれタイトルコードがＴ１、Ｔ２、Ｔ３の暗号化コンテンツを復号するための復号鍵である。

【０１３８】

ＤＩＤ１、ＤＩＤ２、ＤＩＤ３はそれぞれ異なるＣＡＴＶデコーダのシステムＩＤであり、ＢＣＡ１、ＢＣＡ２、ＢＣＡ３はそれぞれ異なる光ディスクのディスクＩＤである。

【０１３９】

このとき、ＣＡＴＶデコーダに入力される鍵Ｋｍｎは、ＦＫｎ＝Ｋｍｎ＊Ｔｎ＊ＤＩＤ＊ＴＩＭＥｎを満足するように決定され、光ディスク記録装置に入力される鍵ＤＫは、ＦＫｎ＝ＤＫｍｎ＊ＢＣＡｍ＊Ｔｎを満足するように決定される。

【０１４０】

図８に示す様に、コンテンツが異なるときはもちろんのこと、コンテンツが同じ場合でも、異なるＣＡＴＶデコーダ、異なるディスク、異なる放送時間ごとに鍵発行センターから入手する鍵情報は異なることから細部にわたる著作権の保護が可能になる。

【０１４１】

同様に、コンテンツが同じでもシステムＩＤ、ディスクＩＤ、時間情報が異なれば鍵情報が異なることから、ＣＡＴＶ会社７０１は、ユーザごとに暗号化コンテンツを変える必要がなく、１つのコンテンツに対して１つの暗号化コンテンツを準備すれば良い。これにより放送時のシステムを簡単にでき、低コストで、大量の視聴者へのコンテンツの提供が可能になる。

【０１４２】

なお本実施の形態ではケーブルテレビからのコンテンツを放送する場合について説明したが、電波による放送でも同様である。

【０１４３】

【発明の効果】

本実施の形態の書き換え型もしくは追記型の光ディスクにより、従来の光ディスクに、前記光ディスクを識別する情報を付加することで、光ディスクの管理を容易に実現することができる。

【０１４４】

また本実施の形態の暗号化データの記録方法により、世の中に１枚しか存在しない、光ディスクを識別する情報により暗号化することにより、光ディスクの不正なコピーを防止し、１枚の光ディスクにしか同じ暗号化コンテンツの記録ができないため、著作権が保護できるという効果がある。

【０１４５】

また本実施の形態の書き換え型もしくは追記型の光ディスクにより、暗号化されて記録されたデータを解読する際に鍵情報が必要なシステムにおいて、鍵情報記録領域に鍵情報が一度記録されることにより、再生する度に鍵情報を入手する必要がなくなるという効果がある。

【０１４６】

また本実施の形態の暗号化データの記録方法により、暗号化されたコンテンツをコピーされても、不正に再生されることはなく、さらに復号化されたコンテンツが複製される際には必ず課金が伴うことから著作権を保護することができる。

【０１４７】

また本実施の形態の暗号化データの記録方法により、コンテンツが同じでもシステムＩＤ、ディスクＩＤ、時間情報が異なれば鍵情報が異なることから、ＣＡＴＶ会社７０１は、ユーザごとに暗号化コンテンツを変える必要がなく、１つのコンテンツに対して１つの暗号化コンテンツを準備すれば良く、これにより放送時のシステムを簡単にでき、低コストで、大量の視聴者へのコンテンツの提供が可能になる。

【図面の簡単な説明】

【図１】

本発明の第１の実施の形態における光ディスクの平面図

【図２】

本発明の第１の実施の形態におけるＢＣＡ領域を再生したときの光ディスク記録装置の出力信号の説明図

【図３】

本発明の第１の実施の形態におけるＢＣＡ再生部のブロック図

【図４】

本発明の第１の実施の形態における暗号化コンテンツの記録方法のブロック図

【図５】

本発明の第２の実施の形態における暗号化コンテンツの記録方法のブロック図

【図６】

本発明の第３の実施の形態における光ディスクの平面図

【図７】

本発明の第３の実施の形態における暗号化コンテンツの記録方法のブロック図

【図８】

本発明の第３の実施の形態における、システムＩＤ、ディスクＩＤが異なる場合の鍵情報の整理のための図

【符号の説明】

１０１　光ディスク

１０２　コントロールデータ領域

１０３　データ領域

１０４　ＢＣＡ領域

３０１　光ピック

４０１　ＢＣＡ再生部

４０８　暗号化エンコーダ

４１２　データ再生部

４１３　暗号デコーダ

５０８　システムＩＤ

５２３　会社識別信号

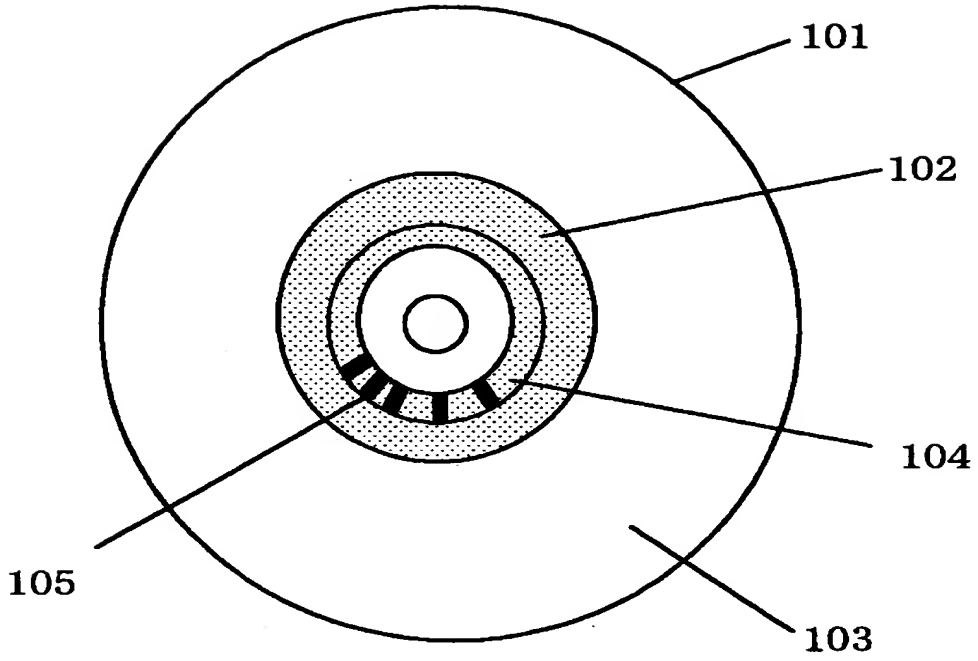
６０５　鍵情報記録領域

７１９　鍵情報記録回路

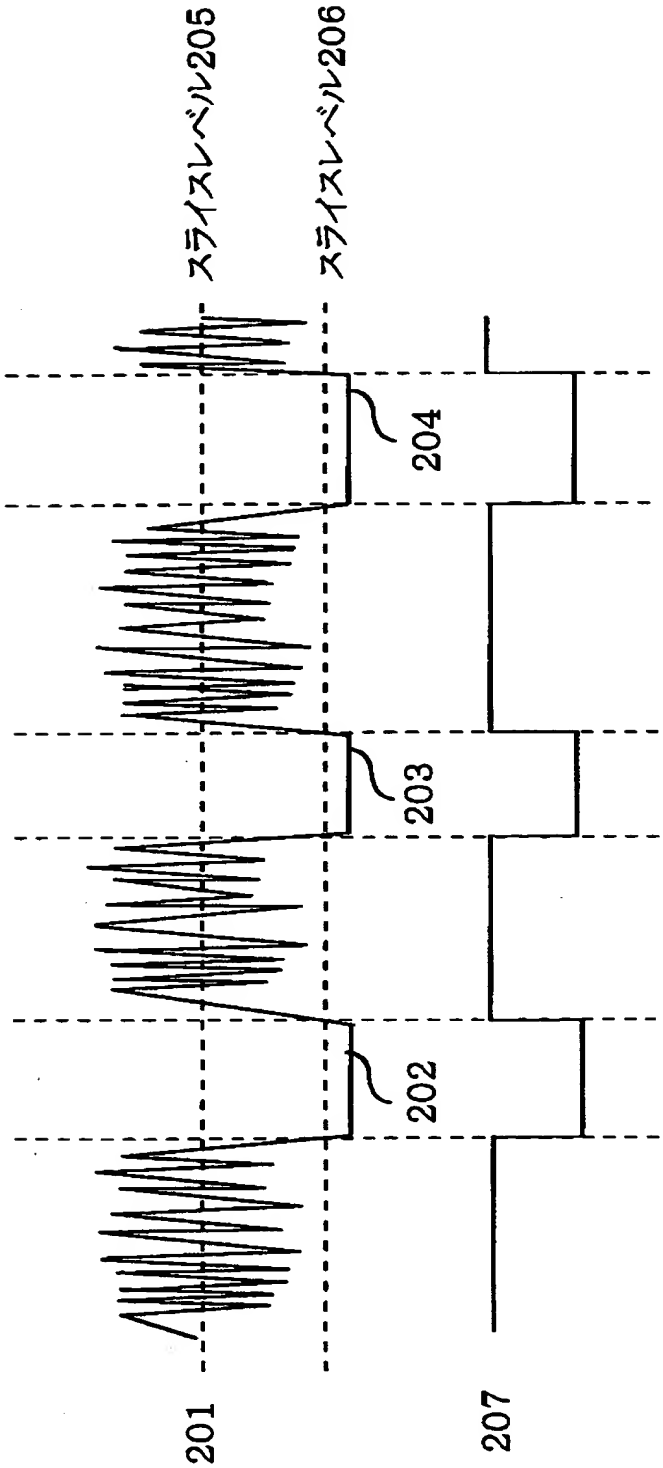
７２３　鍵情報再生部

【書類名】　　図面

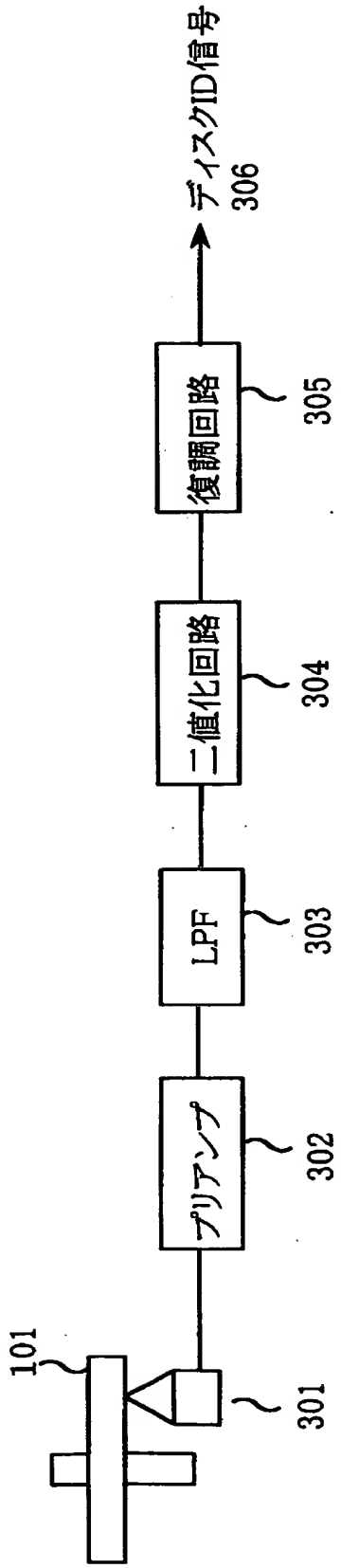
【図１】



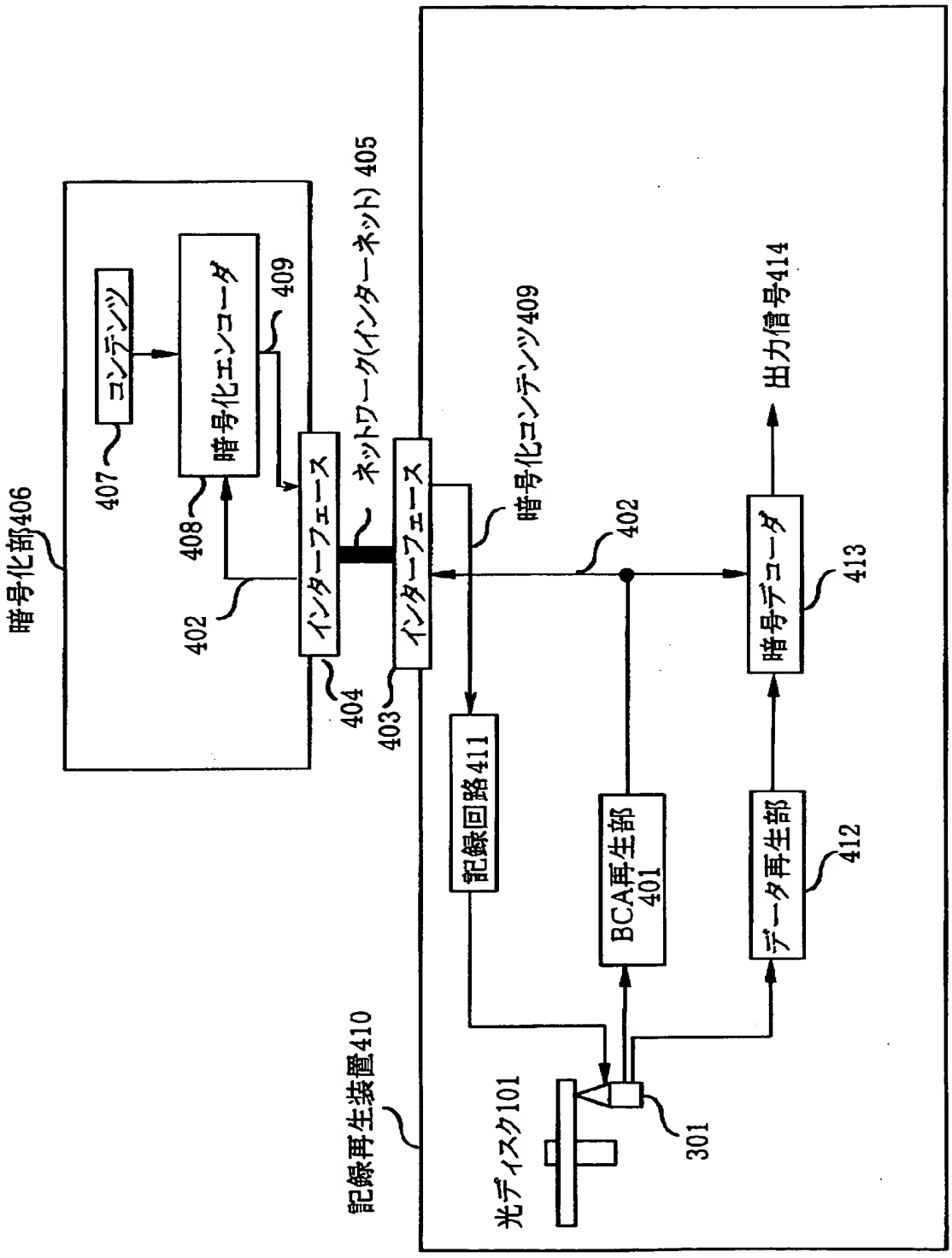
【図２】



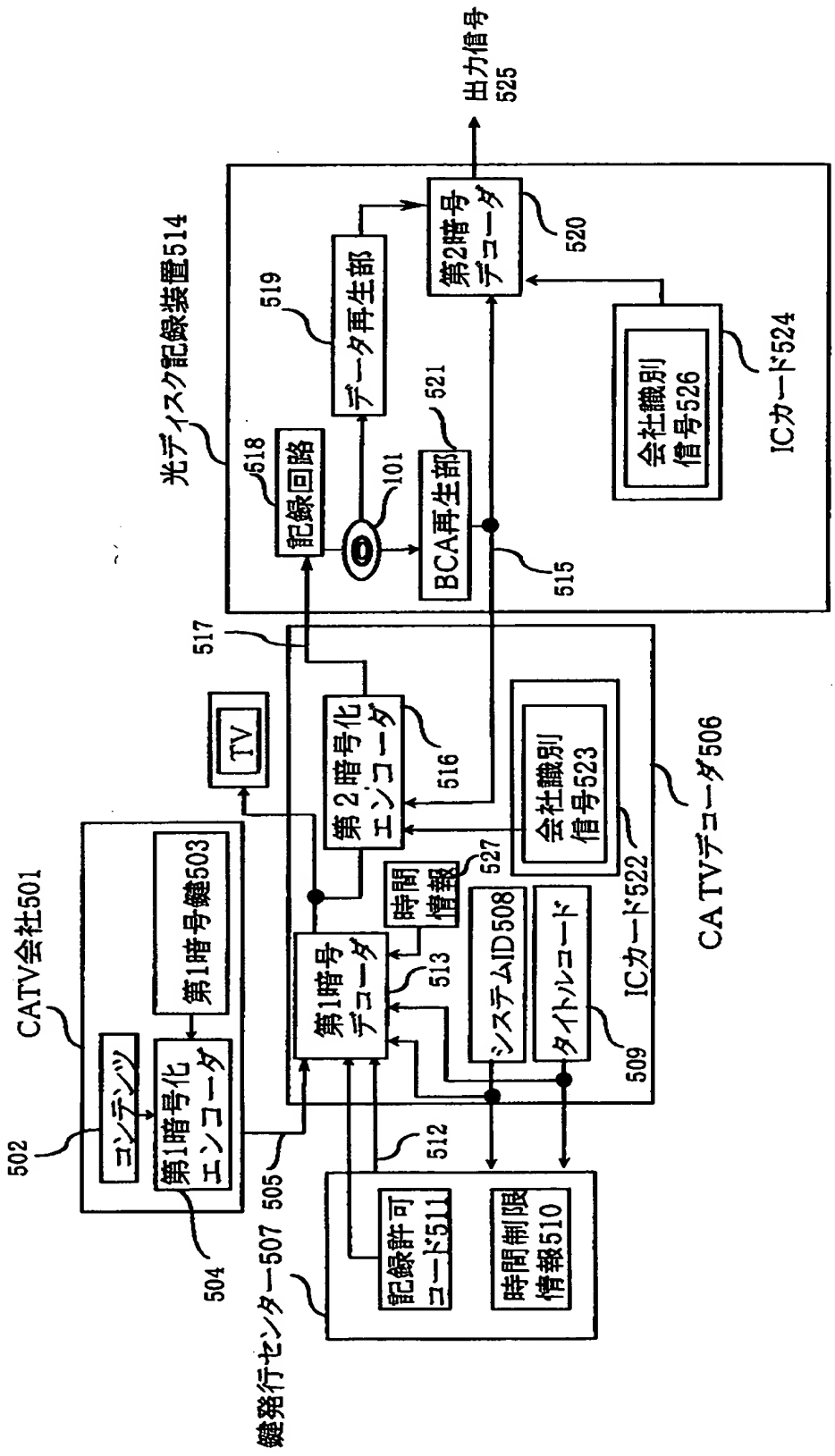
【図３】



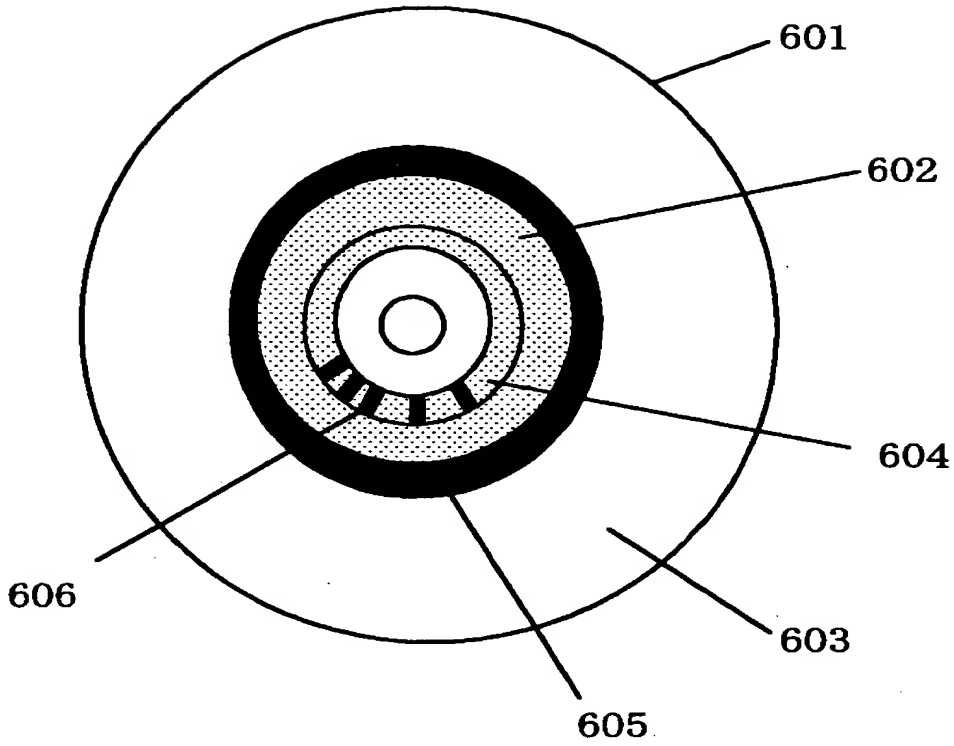
【図４】


暗号化部406
コンテンツ
407
暗号化エンコーダ
408
409
402
インターフェース
404
ネットワーク(インターネット) 405
インターフェース
403
暗号化コンテンツ409
402
出力信号414
暗号デコーダ
413
記録回路411
BCA再生部
401
データ再生部
412
記録再生装置410
光ディスク101
301

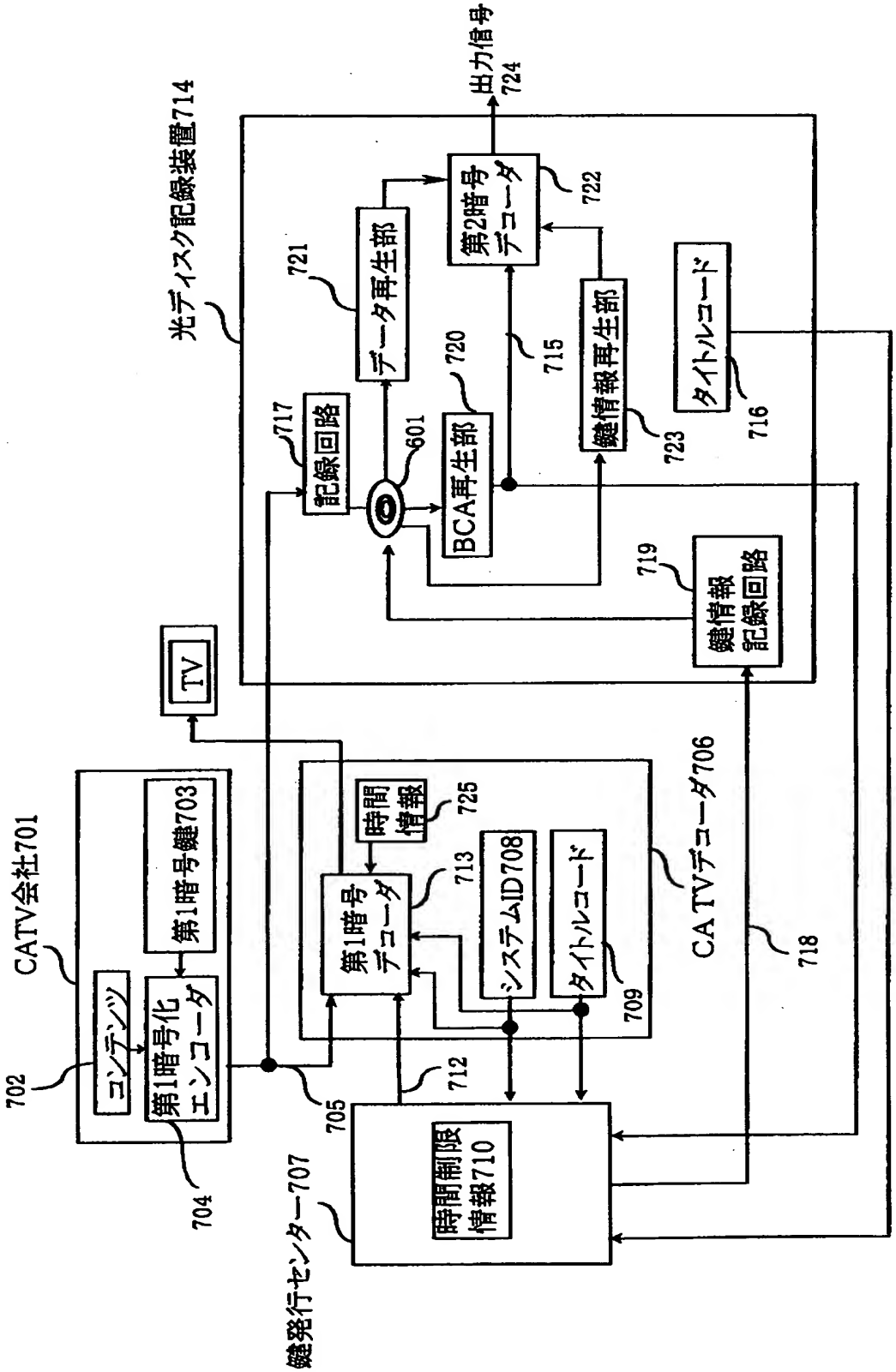
【図５】


出力信号
525
光ディスク記録装置514
519
データ再生部
520
第2暗号
デコーダ
518
記録回路
101
521
BCA再生部
515
会社識別
信号526
ICカード524
517
TV
第２暗号化
エンコーダ
516
会社識別
信号523
CA TVデコーダ506
527
時間
情報
513
第1暗号
デコーダ
システムID508
タイトルコード
509
ICカード522
CATV会社501
502
コンテンツ
第1暗号化
エンコーダ
第1暗号鍵503
504
505
512
鍵発行センター507
記録許可
コード511
時間制限
情報510

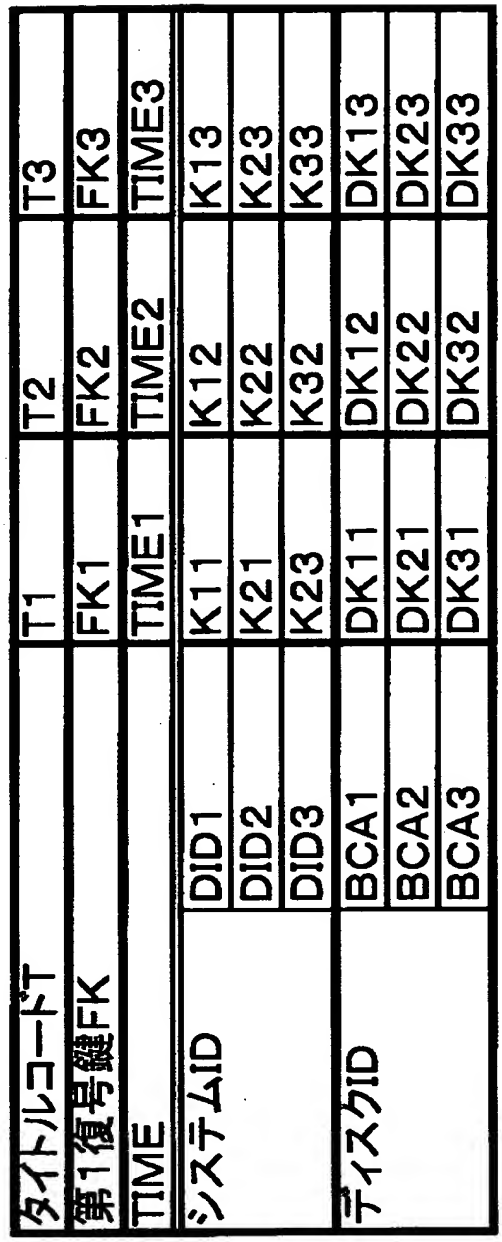
【図６】



【図７】


CATV会社701
ヨンテンツ
第1暗号化エンコーダ
第1暗号鍵703
702
704
705
712
鍵発行センター707
時間制限情報710
第1暗号デコーダ
713
時間情報
725
システムID708
タイトルコード
709
CATVデコーダ706
718
光ディスク記録装置714
TV
記録回路
717
601
データ再生部
721
BCA再生部
720
715
第2暗号デコーダ
722
出力信号
724
鍵情報再生部
723
タイトルコード
716
鍵情報記録回路
719

【図８】


タイトルコードT
第1復号鍵FK
TIME
システムID
DID1
DID2
DID3
ディスクID
BCA1
BCA2
BCA3
T1
FK1
TIME1
K11
K21
K23
DK11
DK21
DK31
T2
FK2
TIME2
K12
K22
K32
DK12
DK22
DK32
T3
FK3
TIME3
K13
K23
K33
DK13
DK23
DK33

【書類名】　要約書

【要約】

【課題】　簡単なシステムで、不正コピーを防止しつつ、ネットワークもしくは電波により発信されたコンテンツを光ディスクへ記録するための、暗号化コンテンツ記録方法を提供することを目的とする。

【解決手段】　ディスクの種類等を凹凸ピットで記録してあるコントロールデータ領域１０２、ユーザがデータを記録するデータ領域１０３、コントロールデータ領域１０２の内周部分の凹凸ピット上の記録膜をＹＡＧレーザなどのパルスレーザでトリミングすることにより、ディスクＩＤ信号を記録してあるＢＣＡ領域１０４を有し、ディスクＩＤ信号が暗号を解く復号鍵となるように暗号化されたコンテンツをデータ領域１０３に記録する。

【選択図】　図１

出　願　人　履　歴　情　報

識別番号　　〔０００００５８２１〕

１．変更年月日　　１９９０年　８月２８日
［変更理由］　新規登録
住　所　　大阪府門真市大字門真１００６番地
氏　名　　松下電器産業株式会社